THE ROSEN LAW FIRM, P.A.
Phillip Kim, Esq.
Laurence M. Rosen, Esq.
275 Madison Avenue, 40th Floor
New York, New York 10016
Telephone: (212) 686-1060
Fax: (212) 202-3827
Email: philkim@rosenlegal.com
Email: lrosen@rosenlegal.com

Counsel for Plaintiff

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

BLAKE BAXTER, Individually and on behalf of all others similarly situated, Plaintiff, v. PDD HOLDINGS INC. F/K/A PINDUODUO INC., LEI CHEN, JING MA, and JUN LIU, Defendants.	**Case No:** **CLASS ACTION COMPLAINT FOR VIOLATIONS OF THE FEDERAL SECURITIES LAWS** JURY TRIAL DEMANDED CLASS ACTION

Plaintiff Blake Baxter ("Plaintiff"), individually and on behalf of all other persons similarly situated, by Plaintiff's undersigned attorneys, for Plaintiff's complaint against Defendants (defined below), alleges the following based upon personal knowledge as to Plaintiff and Plaintiff's own acts, and information and belief as to all other matters, based upon, among other things, the investigation conducted by and through his attorneys, which included, among other things, a review of the Defendants' public documents, public filings, United States Securities and Exchange Commission ("SEC") filings, wire and press releases published by and regarding PDD Holdings Inc. f/k/a Pinduoduo Inc. ("PDD". "PDD Holdings", or the "Company"), and information readily

obtainable on the Internet. Plaintiff believes that substantial evidentiary support will exist for the allegations set forth herein after a reasonable opportunity for discovery.

NATURE OF THE ACTION

1. This is a class action on behalf of persons or entities who purchased or otherwise acquired publicly traded PDD securities between April 30, 2021 and June 25, 2024, inclusive (the "Class Period"). Plaintiff seeks to recover compensable damages caused by Defendants' violations of the federal securities laws under the Securities Exchange Act of 1934 (the "Exchange Act").

JURISDICTION AND VENUE

2. The claims asserted herein arise under and pursuant to Sections 10(b) and 20(a) of the Exchange Act (15 U.S.C. §§ 78j(b) and 78t(a)) and Rule 10b-5 promulgated thereunder by the SEC (17 C.F.R. § 240.10b-5).

3. This Court has jurisdiction over the subject matter of this action pursuant to 28 U.S.C. § 1331, and Section 27 of the Exchange Act (15 U.S.C. §78aa).

4. Venue is proper in this judicial district pursuant to 28 U.S.C. § 1391(b) and Section 27 of the Exchange Act (15 U.S.C. § 78aa(c)) as the alleged misstatements entered and the subsequent damages took place in this judicial district.

5. The Company has submitted to personal jurisdiction in the City of New York. The Company's latest annual report, filed with the SEC on Form 20-F on April 25, 2024, stated that, as per the Company's deposit agreements, federal or state courts in the City of New York have exclusive jurisdiction to hear determine claims arising under its deposit agreements. It specifically stated the following:

> ***ADSs holders may not be entitled to a jury trial with respect to claims arising under the deposit agreements, which could result in less favorable outcomes to the plaintiff(s) in any such action.***

> The deposit agreements governing the ADSs representing our ordinary shares provide that, subject to the depositary's right to require a claim to be submitted to arbitration, ***the federal or state courts in the City of New York have exclusive jurisdiction to hear and determine claims arising under the deposit agreements and in that regard, to the fullest extent permitted by law, ADS holders waive the right to a jury trial of any claim they may have against us or the depositary arising out of or relating to our shares, the ADSs or the deposit agreements, including any claim under the U.S. federal securities laws***.
>
> (Emphasis added).

6. In connection with the acts, conduct and other wrongs alleged in this complaint, Defendants (defined below), directly or indirectly, used the means and instrumentalities of interstate commerce, including but not limited to, the United States mails, interstate telephone communications and the facilities of the national securities exchange.

PARTIES

7. Plaintiff, as set forth in the accompanying certification, incorporated by reference herein, purchased PDD securities during the Class Period and was economically damaged thereby.

8. PDD purports to be "a multinational commerce group that owns and operates a portfolio of businesses." The Company changed its name to PDD Holdings Inc. in February 2023.

9. The Company describes its Pinduoduo platform as follows:

> Our Pinduoduo platform provides buyers with a comprehensive selection of value-for-money merchandise and fun and interactive shopping experiences. The platform pioneered an innovative "team purchase" model. Buyers are encouraged to share product information on social networks, and invite their friends, family and social contacts to form shopping teams to enjoy the more attractive prices available under the "team purchase" option. Pinduoduo's buyer base helps attract merchants to the platform, while the scale of the platform's sales volume encourages merchants to offer more competitive prices and customized products and services to buyers, thus forming a virtuous cycle.

10. The Company describes its Temu platform as follows:

> Temu was founded in September 2022 in Boston, Massachusetts, the United States. As a new initiative at an early stage of development, Temu aspires to become a global online platform dedicated to providing quality products to consumers at attractive prices. In partnership with a global network of logistics vendors and fulfillment partners, Temu empowers merchants with value-added services that enables a broader market reach.

11. The Company is incorporated in the Cayman Islands and its principal place of business is located at First Floor, 25 St Stephen's Green, Dublin 2, D02 XF99 Ireland. It conducts its businesses through operating entities in various jurisdictions around the world.

12. PDD's American Depositary Shares ("ADS" or "ADSs") trade on the NASDAQ exchange under the ticker symbol "PDD."

13. Defendant Lei Chen ("Chen") served as the Company's Chief Executive Officer ("CEO") from July 2020 through April 2023, and since then as co-CEO. Chen is also the current chairman of the Board of Directors (the "Board").

14. Defendant Jing Ma ("Ma") served as the Company's Vice President of Finance from the beginning of the Class Period until January 1, 2022.

15. Defendant Jun Liu ("Liu") has served as the Company's Vice President of Finance from January 2022 to the present.

16. Defendants Chen, Ma, and Liu are collectively referred to herein as the "Individual Defendants."

17. Each of the Individual Defendants:

(a) directly participated in the management of the Company;

(b) was directly involved in the day-to-day operations of the Company at the highest levels;

(c) was privy to confidential proprietary information concerning the Company and its business and operations;

(d) was directly or indirectly involved in drafting, producing, reviewing and/or disseminating the false and misleading statements and information alleged herein;

(e) was directly or indirectly involved in the oversight or implementation of the Company's internal controls;

(f) was aware of or recklessly disregarded the fact that the false and misleading statements were being issued concerning the Company; and/or

(g) approved or ratified these statements in violation of the federal securities laws.

18. The Company is liable for the acts of the Individual Defendants and its employees under the doctrine of *respondeat superior* and common law principles of agency because all of the wrongful acts complained of herein were carried out within the scope of their employment.

19. The scienter of the Individual Defendants and other employees and agents of the Company is similarly imputed to PDD under *respondeat superior* and agency principles.

20. Defendant PDD and the Individual Defendants are collectively referred to herein as "Defendants."

SUBSTANTIVE ALLEGATIONS
Materially False and Misleading Statements Issued During the Class Period

21. On April 30, 2021, the Company filed with the SEC its Annual Report on Form 20-F for the year ended December 31, 2020 (the "2020 Annual Report"). Attached to the 2020 Annual Report were signed certifications pursuant SOX signed by Defendant Chen and Ma attesting to the accuracy of financial reporting, the disclosure of any material changes to the Company's internal controls over financial reporting, and the disclosure of all fraud.

22. The 2020 Annual Report contained the following risk disclosure about the Company's brand and reputation:

> We believe that the recognition and reputation of our Pinduoduo or "拼多多" brand among our buyers, merchants and third-party service providers have contributed significantly to the growth and success of our business. ***Maintaining and enhancing the recognition and reputation of our brand are critical to our business and competitiveness***. Many factors, some of which are beyond our control, are important to maintaining and enhancing our brand. These factors include our ability to:

* * *

- preserve our reputation and goodwill in the event of any negative publicity on our consumer experience or merchant service, ***internet and data security,*** product quality, price or authenticity, performance measures, or other issues affecting us or other e-commerce businesses in China.

(Emphasis added).

23. The statement in ¶ 22 was materially false and misleading at the time it was made because the Company, through its applications, actively sought to put malware on its user's phones. Accordingly, there was a risk of reputational damage if its activities relating to malware were discovered.

24. The 2020 Annual Report contained the following risk disclosure about the improper use of data:

> ***Our business generates and processes a large amount of data, and we are required to comply with PRC and other applicable laws relating to privacy and cyber security. The improper use or disclosure of data could have a material and adverse effect on our business and prospects.***
>
> Our business generates and processes a large quantity of data. We face risks inherent in handling and protecting large volume of data. In particular, we face a number of challenges relating to data from transactions and other activities on our platforms, including:
>
> - protecting the data in and hosted on our system, including against attacks on our system by outside parties or fraudulent behavior ***or improper use by our employees;***
> - addressing concerns related to privacy and sharing, safety, security and other factors; and
> - ***complying with applicable laws, rules and regulations relating to the collection, use, storage, transfer, disclosure and security of personal information***, including any requests from regulatory and government authorities relating to these data.
>
> * * *
>
> In addition, regulatory authorities around the world have recently adopted or are considering a number of legislative and regulatory proposals concerning data protection. These legislative and regulatory proposals, if adopted, and the uncertain interpretations and application thereof could, in addition to the possibility of fines, result in an order requiring

that we change our data practices and policies, which could have an adverse effect on our business and results of operations.

Furthermore, we expect that data security and data protection compliance will receive greater attention and focus from regulators, as well as attract continued or greater public scrutiny and attention going forward, which could increase our compliance costs and subject us to heightened risks and challenges associated with data security and protection. If we are unable to manage these risks, we could become subject to penalties, including fines, suspension of business and revocation of required licenses, and our reputation and results of operations could be materially and adversely affected.

(Emphasis added).

25. The statement in ¶ 24 was materially false and misleading at the time it was made because the Company sought to place malware on its user's smart phones in order to improperly collect personal data, exposing the Company to heightened regulatory risk.

26. The 2020 Annual Report contained the following risk disclosure regarding the failure to protect confidential information:

Failure to protect confidential information of buyers, merchants and our network against security breaches could damage our reputation and brand and substantially harm our business and results of operations.

A significant challenge to the e-commerce industry is the secure storage of confidential information and its secure transmission over public networks. A majority of the orders and the payments for products offered on our platform are made through our mobile app. In addition, all online payments for products sold on our platform are settled through third-party online payment services. ***Maintaining complete security on our platform and systems for the storage and transmission of confidential or private information, such as buyers' personal information, payment-related information and transaction information, is essential to maintain consumer confidence in our platform and systems.***

We have adopted strict security policies and measures, including encryption technology, to protect our proprietary data and buyer information. However, advances in technology, the expertise of hackers, new discoveries in the field of cryptography or other events or developments could result in a compromise or breach of the technology that we use to protect confidential information. We may not be able to prevent third parties, especially hackers or other individuals or entities engaging in similar activities through viruses, Trojan horses, malicious software, break-ins, phishing attacks, third-party manipulation or security breaches, from illegally obtaining such confidential or private information we hold with respect to buyers and merchants on our platform. Such individuals or entities obtaining confidential or private information may further engage in various other illegal

> activities using such information. The methods used by hackers and others engaging in illegal online activities are increasingly more sophisticated and constantly evolving. Significant capital, managerial and other resources, including costs incurred to deploy additional personnel and develop network protection technologies, train employees, and engage third-party experts and consultants, may be required to ensure and enhance information security or to address the issues caused by such security failure.
>
> In addition, we have limited control or influence over the security policies or measures adopted by third-party providers of online payment services through which some of our buyers may choose to make payment for purchases. Any negative publicity on our platform's safety or privacy protection mechanisms and policies, and any claims asserted against us or fines imposed upon us as a result of actual or perceived failures, could have a material and adverse effect on our public image, reputation, financial condition and results of operations. Any compromise of our information security or the information security measures of our contracted third-party online payment service providers could have a material and adverse effect on our reputation, business, prospects, financial condition and results of operations.
>
> (Emphasis added).

27. The statement in ¶ 26 was materially false and misleading because it discussed risks relating to outside parties improperly accessing private confidential information, without disclosing that the Company had sought to improperly obtain data off of its customer's smart phones.

28. The 2020 Annual Report contained the following risk disclosure about scrutiny of the Company:

> ***We may increasingly become a target for public scrutiny, including complaints to regulatory agencies, negative media coverage, and public dissemination of malicious reports or accusations about our business, all of which could severely damage our reputation and materially and adversely affect our business and prospects.***
>
> We process an extremely large number of transactions on a daily basis on our platform, and the high volume of transactions taking place on our platform as well as publicity about our business create the possibility of heightened attention from the public, regulators and the media. Heightened regulatory and public concerns over consumer protection and consumer safety issues may subject us to additional legal and social responsibilities and increased scrutiny and negative publicity over these issues, due to the large number of transactions that take place on our platform and the increasing scope of our overall business operations. In addition, changes in our services or policies have resulted and could result in objections by members of the public, the traditional, new and social media, social

> network operators, merchants on our platform or others. From time to time, these objections or allegations, regardless of their veracity, may result in consumer dissatisfaction, public protests or negative publicity, which could result in government inquiry or substantial harm to our brand, reputation and operations.
>
> Moreover, as our business expands and grows, both organically and through acquisitions of and investments in other businesses, domestically and internationally, we may be exposed to heightened public scrutiny in jurisdictions where we already operate as well as in new jurisdictions where we may operate. There is no assurance that we would not become a target for regulatory or public scrutiny in the future or that scrutiny and public exposure would not severely damage our reputation as well as our business and prospects.

29. The statement in ¶ 28 was materially false and misleading at the time it was made because it stated that the Company could become a target as a result of its scale. In fact, the Company was at increased risk of regulatory and public scrutiny (as well as negative media coverage) due to its malfeasance, including placing malware on its user's smart phones and selling goods that were likely made by forced labor.

30. On April 25, 2022, the Company filed with the SEC its Annual Report on Form 20-F for the year ended December 31, 2021 (the "2021 Annual Report"). Attached to the 2021 Annual Report were signed certifications pursuant SOX signed by Defendants Chen and Liu attesting to the accuracy of financial reporting, the disclosure of any material changes to the Company's internal controls over financial reporting, and the disclosure of all fraud.

31. The 2021 Annual Report Annual Report contained the following risk disclosure about the Company's brand and reputation:

> ***Any harm to our brand or reputation may materially and adversely affect our business and results of operations.***
>
> We believe that the recognition and reputation of our Pinduoduo or "拼多多" brand among our buyers, merchants and third-party service providers have contributed significantly to the growth and success of our business. Maintaining and enhancing the recognition and reputation of our brand are critical to our business and competitiveness. Many factors, some of which are beyond our control, are important to maintaining and enhancing our brand. These factors include our ability to:

* * *

- preserve our reputation and goodwill in the event of any negative publicity on our consumer experience or merchant service, ***internet and data security***, product quality, price or authenticity, performance measures, or other issues affecting us or other e-commerce businesses in China.

(Emphasis added).

32. The statement in ¶ 31 was materially false and misleading at the time it was made because the Company, through its applications, actively sought to put malware on its user's phones. Accordingly, there was a risk of reputational damage if its activities relating to malware were discovered.

33. The 2021 Annual Report contained the following risk disclosure about the improper use of data:

> ***Our business generates and processes a large amount of data, and we are required to comply with PRC and other applicable laws relating to privacy and cybersecurity. The improper use or disclosure of data could have a material and adverse effect on our business and prospects.***
>
> Our business generates and processes a large amount of data. We face risks inherent in handling and protecting them. In particular, we face a number of challenges relating to data from transactions and other activities on our platforms, including:
>
> - protecting the data in and hosted on our system, including against attacks on our system by outside parties or fraudulent behavior ***or improper use by our employees***;
> - addressing concerns related to privacy and sharing, safety, security and other factors; and
> - ***complying with applicable laws and regulations relating to the collection, use, storage, transfer, disclosure and security of personal data***, including any requests from regulatory and government authorities relating to these data.
>
> * * *
>
> In addition to regulations in the PRC, regulatory authorities around the world have adopted or are considering a number of legislative and regulatory proposals concerning data protection. These legislative and regulatory proposals, if adopted, and the uncertain interpretations and application thereof could, in addition to the possibility of fines, result in an order requiring that we change our data practices and policies, which could have an adverse effect on our business and results of operations. For example, the European Union General Data Protection Regulation ("GDPR"), which came into effect on May 25, 2018, includes operational requirements for companies that receive or process personal data of residents of the European Economic Area. The GDPR establishes new requirements

> applicable to the processing of personal data, affords new data protection rights to individuals and imposes penalties for serious data breaches. Individuals also have a right to compensation under the GDPR for financial or non-financial losses. Although we do not conduct any business in the European Economic Area, in the event that residents of the European Economic Area access our website or our mobile platform and input protected information, we may become subject to provisions of the GDPR.
>
> (Emphasis added).

34. The statement in ¶ 33 was materially false and misleading at the time it was made because the Company placed malware on its user's smart phones in order to improperly collect personal data, exposing the Company to heightened regulatory risk.

35. The 2021 Annual Report contained the following risk disclosure regarding the failure to protect confidential information:

> A significant challenge to the e-commerce industry is the secure storage of confidential information and its secure transmission over public networks. A majority of the orders and the payments for products offered on our platform are made through our mobile app. In addition, all online payments for products sold on our platform are settled through third-party online payment services. ***Maintaining complete security on our platform and systems for the storage and transmission of confidential or private information, such as buyers' personal information, payment-related information and transaction information, is essential to maintain consumer confidence in our platform and systems***.
>
> ***We have adopted strict security policies and measures, including encryption technology, to protect our proprietary data and buyer information. However, advances in technology, the expertise of hackers, new discoveries in the field of cryptography or other events or developments could result in a compromise or breach of the technology that we use to protect confidential information***. We may not be able to prevent third parties, especially hackers or other individuals or entities engaging in similar activities through viruses, Trojan horses, malicious software, break-ins, phishing attacks, third-party manipulation or security breaches, from illegally obtaining such confidential or private information we hold with respect to buyers and merchants on our platform. Such individuals or entities obtaining confidential or private information may further engage in various other illegal activities using such information. The methods used by hackers and others engaging in illegal online activities are increasingly more sophisticated and constantly evolving. Significant capital, managerial and other resources, including costs incurred to deploy additional personnel and develop network protection technologies, train employees, and engage third-party experts and consultants, may be required to ensure and enhance information security or to address the issues caused by such security failure.

> In addition, we have limited control or influence over the security policies or measures adopted by third-party providers of online payment services through which some of our buyers may choose to make payment for purchases. Any negative publicity on our platform's safety or privacy protection mechanisms and policies, and any claims asserted against us or fines imposed upon us as a result of actual or perceived failures, could have a material and adverse effect on our public image, reputation, financial condition and results of operations. Any compromise of our information security or the information security measures of our contracted third-party online payment service providers could have a material and adverse effect on our reputation, business, prospects, financial condition and results of operations.
>
> (Emphasis added).

36. The statement in ¶ 35 was materially false and misleading because it discussed risks relating to outside parties improperly accessing private confidential information, without disclosing that the Company had sought to improperly obtain data off of its customer's smart phones.

37. The 2021 Annual Report contained the following risk disclosure about scrutiny of the Company:

> ***We may increasingly become a target for public scrutiny, including complaints to regulatory agencies, negative media coverage, and public dissemination of malicious reports or accusations about our business, all of which could severely damage our reputation and materially and adversely affect our business and prospects.***
>
> We process an extremely large number of transactions on a daily basis on our platform, and the high volume of transactions taking place on our platform as well as publicity about our business create the possibility of heightened attention from the public, regulators and the media. Heightened regulatory and public concerns over consumer protection and consumer safety issues may subject us to additional legal and social responsibilities and increased scrutiny and negative publicity over these issues, due to the large number of transactions that take place on our platform and the increasing scope of our overall business operations. In addition, changes in our services or policies have resulted and could result in objections by members of the public, the traditional, new and social media, social network operators, merchants on our platform or others. From time to time, these objections or allegations, regardless of their veracity, may result in consumer dissatisfaction, public protests or negative publicity, which could result in government inquiry or substantial harm to our brand, reputation and operations.
>
> Moreover, as our business expands and grows, both organically and through acquisitions of and investments in other businesses, domestically and internationally, we may be

> exposed to heightened public scrutiny in jurisdictions where we already operate as well as in new jurisdictions where we may operate. There is no assurance that we would not become a target for regulatory or public scrutiny in the future or that scrutiny and public exposure would not severely damage our reputation as well as our business and prospects.

38. The statement in ¶ 37 was materially false and misleading at the time it was made because it stated that the Company could become a target as a result of its scale. In fact, the Company was at increased risk of regulatory and public scrutiny (as well as negative media coverage) due to its malfeasance, including placing malware on its user's smart phones and selling goods that were likely made by forced labor.

39. The 2021 Annual Report contained the following risk disclosure regarding international trade policies:

> ***Changes in U.S. and international trade policies, particularly with regard to China, may adversely impact our business and operating results.***
>
> The U.S. government has recently proposed, among other actions, imposing new or higher tariffs on specified products imported from China to penalize China for what it characterizes as unfair trade practices and China has responded by proposing new or higher tariffs on specified products imported from the United States. For example, in 2018, the United States announced three finalized tariffs that applied exclusively to products imported from China, totaling approximately US$250 billion, and in May 2019 the United States increased from 10% to 25% the rate of certain tariffs previously levied on Chinese products. Trade tension between China and the United States may intensify, and the United States may adopt even more drastic measures in the future. Although cross-border business may not be an area of our focus, if we plan to sell our products internationally in the future, any unfavorable government policies on international trade, such as capital controls or tariffs, may affect the demand for our products and services, impact the competitive position of our products or prevent us from being able to sell products in certain countries. If any new tariffs, legislation and/or regulations are implemented, or if existing trade agreements are renegotiated such changes could have an adverse effect on our business, financial condition, results of operations. In addition, future actions or escalations by either the United States or China that affect trade relations may cause global economic turmoil and potentially have a negative impact on our business.
>
> In addition, recent economic and trade sanctions threatened and/or imposed by the U.S. government on a number of China-based technology companies have raised concerns as to whether, in the future, there may be additional regulatory challenges or enhanced restrictions involving other China-based technology companies in areas such as data security, information technology or other business activities. Similar or more expansive

> restrictions that may be imposed by the U.S. or other jurisdictions in the future, may materially and adversely affect our ability to acquire technologies, systems or devices that may be important to our technology infrastructure, service offerings and business operations.

40. The statement in ¶ 39 was materially false and misleading at the time it was made because, by the time the 2021 Annual Report was filed with the SEC, President Joe Biden had signed into law the Uyghur Forced Labor Prevention Act (the "UFLPA"). Under the UFLPA, products originating from the Xinjiang region of China imported into the United States must be certified as not being produced by forced labor. Given that the Company shipped goods into the United States from Xinjiang, the UFLPA presented increased risk.

41. On April 26, 2023, and the Company filed with the SEC its Annual Report on Form 20-F for the year ended December 31, 2022 (the "2022 Annual Report"). Attached to the 2022 Annual Report were signed certifications pursuant SOX signed by Defendants Chen and Liu attesting to the accuracy of financial reporting, the disclosure of any material changes to the Company's internal controls over financial reporting, and the disclosure of all fraud.

42. The 2022 Annual Report Annual Report contained the following risk disclosure about the Company's brand and reputation:

> ***Any harm to our brands or reputation may materially and adversely affect our business and results of operations.***
>
> We believe that the recognition and reputation of our brands, including Pinduoduo and Temu, among our buyers, merchants and third-party service providers have contributed significantly to the growth and success of our business. Maintaining and enhancing the recognition and reputation of our brands are critical to our business and competitiveness.
>
> Many factors, some of which are beyond our control, are important to maintaining and enhancing our brands. These factors include our ability to:
>
> * * *
>
> - preserve our reputation and goodwill in the event of any negative publicity on our consumer experience or merchant service, ***internet and data security***, product

> quality, price or authenticity, performance measures, or other issues affecting us or other e-commerce businesses in the countries or regions where we have operations.
>
> * * *
>
> If we are unable to maintain our reputation, enhance our brand recognition or increase positive awareness of our platforms, products and services, it may be difficult to maintain and grow our buyer base, and our business and growth prospects may be materially and adversely affected.

(Emphasis added).

43. The statement in ¶ 42 was materially false and misleading at the time it was made because the Company, through its applications, actively sought to put malware on its user's phones. Accordingly, there was a risk of reputational damage if its activities relating to malware were discovered.

44. The 2022 Annual Report contained the following risk disclosure about the improper use of data:

> ***Our business generates and processes a large amount of data, and we are required to comply with applicable laws relating to privacy and cybersecurity. The improper use or disclosure of data could have a material and adverse effect on our business and prospects.***
>
> Our business generates and processes a large amount of data. We face risks inherent in handling and protecting them. In particular, we face a number of challenges relating to data from transactions and other activities on our platforms, including:
>
> - protecting the data in and hosted on our system, including against attacks on our system by outside parties ***or fraudulent behavior or improper use by our employees***, and securely transmitting such data over public networks;
> - addressing concerns related to privacy and sharing, ***safety, security and other factors***; and
> - complying with applicable laws and regulations relating to the collection, use, storage, transfer, disclosure and security of personal data, including requests from regulatory and government authorities relating to these data.
>
> To address these challenges, we have adopted strict security policies and measures, including encryption technology, to protect our proprietary data and buyer information. ***Maintaining complete security on our platforms and systems for the storage and transmission of confidential or private data, such as buyers' personal information, payment-related information and transaction information, is essential to maintain consumer confidence in our platforms and systems.***

> However, advances in technology, the expertise of hackers, new discoveries in the field of cryptography or other events or developments could result in a compromise or breach of the technology that we use to protect our data. We may not be able to prevent third parties, especially hackers or other individuals or entities engaging in similar activities through viruses, Trojan horses, malicious software, break-ins, phishing attacks, third-party manipulation or security breaches, from illegally obtaining the confidential or private data we hold on our platforms. Individuals or entities that illegally obtain confidential or private data may further engage in various other illegal activities using such data. The methods used by hackers and others engaging in illegal online activities are increasingly more sophisticated and constantly evolving. In addition, all online payments for products sold on our platforms are settled through third-party online payment services. We have limited control or influence over the security policies or measures adopted by third-party providers of online payment services through which some of our buyers may choose to make payment for purchases.
>
> ***Any negative publicity on our platforms' data safety or privacy protection mechanisms and policies, and any claims asserted against us or fines imposed upon us as a result of actual or perceived failures, could have a material and adverse effect on our public image, reputation, financial condition and results of operations***. Any compromise of our information security or the information security measures of our contracted third-party online payment service providers that results in data being improperly used or disclosed could have a material and adverse effect on our reputation, business, prospects, financial condition and results of operations. Significant capital, managerial and other resources, including costs incurred to deploy additional personnel and develop network protection technologies, train employees, and engage third-party experts and consultants, may be required to ensure and enhance information security or to address the issues caused by a potential security failure.
>
> (Emphasis added).

45. The statement in ¶ 44 was materially false and misleading at the time it was made because it omitted that the Company placed malware on its user's smart phones in order to improperly collect personal data, exposing the Company to heightened regulatory risk.

46. The 2022 Annual Report contained the following risk disclosure about scrutiny of the Company:

> ***We may increasingly become a target for public scrutiny and anti-competitive conducts of competitors or third parties with ill intent, including complaints to regulatory agencies, negative media coverage, and public dissemination of malicious reports or accusations about our business, all of which could severely damage our reputation and materially and adversely affect our business and prospects.***

We process an extremely large number of transactions on a daily basis on our platforms, and the high volume of transactions taking place on our platforms as well as publicity about our business create the possibility of heightened attention from the public, competitors, regulators and the media. Heightened regulatory and public concerns over consumer protection and consumer safety issues may subject us to additional legal and social responsibilities and increased scrutiny and negative publicity over these issues, due to the large number of transactions that take place on our platform and the increasing scope of our overall business operations. In addition, changes in our services or policies have resulted and could result in objections by the public, our competitors, operators of traditional or new media and social networks, merchants on our platform or others. ***From time to time, these objections or allegations, regardless of their veracity, may result in consumer dissatisfaction, public protests or negative publicity, which could result in government inquiry or substantial harm to our brand, reputation and operations***.

In particular, as the competition in the e-commerce industry further intensifies, we are increasingly susceptible to aggressive, anti-competitive and potentially malicious behaviors, conducts and campaigns by our competitors or third parties with ill intent. For example, untrue and unsubstantiated allegations targeting our platforms or merchants on our platforms may be posted on internet forums, social media platforms or websites by anyone on an anonymous basis. The availability of information on the Internet is virtually immediate, as is its impact. These information platforms may not necessarily filter or check the accuracy of information before allowing them to be published. We are often afforded little or no time to respond. For instance, in March 2023, a number of media channels reported cybersecurity concerns about our Pinduoduo mobile app alleged by an anonymous source. Competitors or third parties with ulterior motives could launch aggressive marketing and publicity strategies against us and place the media coverage about this incident among other innocuous or unrelated matters. We are working with stakeholders to refute the allegations while using this opportunity to review our practices. As a result of these anti-competitive conducts, or activities in the similar nature, our brand name and reputation may be materially and adversely affected, and our business operations and strategies may be disrupted or harmed. We may even be subject to governmental or regulatory scrutiny or third-party claims as a result. Meanwhile, we may be required to spend significant amount of time and incur substantial costs to react to or address these consequences. There is no assurance that we will be able to effectively fend ourselves off these anti-competitive conducts within a reasonable period of time, or at all.

Moreover, as our business expands and grows, both organically and through acquisitions of and investments in other businesses, domestically and internationally, we may be exposed to heightened public scrutiny in jurisdictions where we already operate as well as in new jurisdictions where we may operate. There is no assurance that we would not become a target for regulatory or public scrutiny in the future or that scrutiny and public exposure would not severely damage our reputation as well as our business and prospects.

(Emphasis added).

47. The statement in ¶ 46 was materially false and misleading at the time it was made because it stated that the Company could become a target as a result of its scale. In fact, the Company was at increased risk of regulatory and public scrutiny (as well as negative media coverage) due to its malfeasance, including placing malware on its user's smart phones and selling goods that were likely made by forced labor.

48. The 2022 Annual Report contained the following risk disclosure regarding international trade policies:

> ***Changes in U.S. and international trade policies, particularly with regard to China, may adversely impact our business and operating results.***
>
> The U.S. government has proposed, among other actions, imposing new or higher tariffs on specified products imported from China to penalize China for what it characterizes as unfair trade practices and China has responded by proposing new or higher tariffs on specified products imported from the United States. For example, in 2018, the United States announced three finalized tariffs that applied exclusively to products imported from China, totaling approximately US$250 billion, and in May 2019 the United States increased from 10% to 25% the rate of certain tariffs previously levied on Chinese products. ***Trade tension between China and the United States may intensify, and the United States may adopt even more drastic measures in the future. Any unfavorable government policies on international trade, such as capital controls or tariffs, may affect the demand for our products and services, impact the competitive position of our products or prevent us from being able to sell products in certain countries***. If any new tariffs, legislation and/or regulations are implemented, or if existing trade agreements are renegotiated such changes could have an adverse effect on our business, financial condition, results of operations. In addition, future actions or escalations by either the United States or China that affect trade relations may cause global economic turmoil and potentially have a negative impact on our business.
>
> In particular, economic tension between the United States and China, or between other countries, may intensify and the United States, China, or other countries may adopt drastic measures in the future that impact our global expansion and our business. Recent economic and trade sanctions threatened and/or imposed by the U.S. government on a number of technology companies with significant China operations have raised concerns as to whether, in the future, there may be additional regulatory challenges or enhanced restrictions involving other technology companies with significant China operations. Similar or more expansive restrictions that may be imposed by the U.S. or other jurisdictions in the future, may materially and adversely affect our ability to acquire technologies, systems or devices that may be important to our technology infrastructure, service offerings and business operations. The adoption or expansion of restrictions,

> including restrictions on access to apps and other platforms, cross-border data transfers, tariffs, or other governmental action related to economic policies, has the potential to adversely impact our business, operational results and financial position.
>
> (Emphasis added).

49. The statement in ¶ 48 was materially false and misleading at the time it was made because, by the time the 2022 Annual Report was filed with the SEC, the UFLPA had been signed and gone into effect. Under the UFLPA, products originating from the Xinjiang region of China imported into the United States must be certified as not being produced by forced labor. Given that the Company shipped goods into the United States from Xinjiang, the UFLPA presented increased risk.

50. The 2022 Annual Report contained the following risk disclosure about legal compliance:

> ***Our business is subject to a large number of laws across many jurisdictions, many of which are evolving.***
>
> We are subject to a variety of laws and regulation around the world, including those relating to traditional businesses, such as employment laws, accessibility requirements, and taxation, and laws and regulations focused on e-commerce and online marketplaces, such as online payments, privacy, anti-spam, data security and protection, online platform liability, marketplace seller regulation, intellectual property, product liability, marketing, and consumer protection.
>
> These laws and regulations are continuously evolving, and compliance is costly and can require changes to our business practices and significant management time and effort. Additionally, it is not always clear how existing laws apply to online marketplaces as many of these laws do not address the unique issues raised by online marketplaces or e-commerce. In some jurisdictions, these laws and regulations subject us to attempts to apply domestic rules worldwide against us, and occasionally may subject us to inconsistent obligations across jurisdictions.
>
> ***We strive to comply with all applicable laws***, but they may conflict with each other, and by complying with the laws or regulations of one jurisdiction, we may find that we are violating the laws or regulations of another jurisdiction. ***Despite our efforts, we may not have fully complied in the past and may not fully comply in the future, particularly where the applicable regulatory regimes have not been broadly interpreted***. If we become liable under laws or regulations applicable to us, we could be required to pay significant fines

> and penalties, our reputation may be harmed, and we may be forced to change the way we operate. That could require us to incur significant expenses or to discontinue certain services, which could negatively affect our business. In addition, if we are restricted from operating in one or more countries, our ability to attract and retain sellers and buyers may be adversely affected and we may not be able to grow our business as we anticipate.
>
> Additionally, if third parties with whom we work violate applicable laws or our policies, those violations could also result in liabilities for us and could harm our business. Our ability to rely on insurance, contracts, indemnification and other remedies to limit these liabilities, may be insufficient or unavailable in some cases. Furthermore, the circumstances in which we may be held liable for the acts, omissions, or responsibilities of our merchants is uncertain, complex, and evolving.
>
> (Emphasis added).

51. The statement in ¶ 50 was materially false and misleading at the time it was made because the Company did not meaningfully attempt to comply with the UFLPA.

52. On February 9, 2024, after the Committee Report's release (discussed below), CNBC published an article entitled "Temu returns to Super Bowl ad slate as lawmaker ire swells." This article discussed a growing backlash to Temu from American lawmakers due to lack of compliance with the UFLPA. CNBC quoted a Temu spokesperson as saying that Temu's standards and practicing surrounding the use of forced labor are "no different" from major e-commerce companies such as "Amazon, eBay, and Etsy" and that allegations against Temu are "completely ungrounded." The CNBC article further quoted the spokesperson as saying the following:

> Before setting up their stores and listing products on Temu, every seller has to sign an agreement. This document stands as a pledge to maintain lawful and compliant business operations, and adhere strictly to the legal standards and regulations of their specific markets[.]
>
> ***The use of forced, penal, or child labor is strictly prohibited***. Employment by all our merchants and suppliers must be strictly voluntary. They shall respect the freedom of association and workers' rights to collectively bargain. Temu's merchants suppliers, and other parties must pay their employees and contractors on time and must comply with all applicable local wage and hours laws.
>
> (Emphasis added).

53. The statement in ¶ 52 was materially false and misleading at the time it was made because, despite whatever boilerplate agreement that Temu had with its suppliers, it did not prohibit suppliers from exporting goods into the United States from Xinjiang in violation of American law, and had no meaningful mechanism to verify that goods shipped into the United States were not made with forced labor.

54. On March 5, 2024, the Financial Times published a documentary film on YouTube entitled "The rise of Pinduoduo and Temu: profits and secrets." This video quoted a Temu as saying the following in response to the discussion of allegations of forced labor:

> Anyone doing business with Temu must strictly comply with all regulatory standards and compliance requirements[.]
>
> We strictly prohibit the use of forced, penal, or child labour[.]
>
> ***Allegations in this regard are completely ungrounded***.
>
> (Emphasis added).

55. The statement in ¶ 54 was materially false and misleading at the time it was made because, despite whatever boilerplate agreement that Temu had with its suppliers, it did not prohibit suppliers from exporting certain goods into the United States from Xinjiang in violation of American law, and had no meaningful mechanism to verify that goods shipped into the United States were not made with forced labor.

56. On April 25, 2024, the Company filed with the SEC its Annual Report on Form 20-F for the year ended December 31, 2023 (the "2023 Annual Report"). Attached to the 2023 Annual Report were signed certifications pursuant SOX signed by Defendants Chen and Liu attesting to the accuracy of financial reporting, the disclosure of any material changes to the Company's internal controls over financial reporting, and the disclosure of all fraud.

57. The 2023 Annual Report Annual Report contained the following risk disclosure about the Company's brand and reputation:

> ***Any harm to our brands or reputation may materially and adversely affect our business and results of operations.***
>
> We believe that the recognition and reputation of our brands, including Pinduoduo and Temu, among our buyers, merchants and third-party service providers have contributed significantly to the growth and success of our business. Maintaining and enhancing the recognition and reputation of our brands are critical to our business and competitiveness.
>
> Many factors, some of which are beyond our control, are important to maintaining and enhancing our brands. These factors include our ability to:
>
> * * *
>
> - preserve our reputation and goodwill in the event of any negative publicity on our consumer experience or merchant service, ***internet and data security***, product quality, price or authenticity, performance measures, or other issues affecting us or other e-commerce businesses in the countries or regions where we have operations.

(Emphasis added).

58. The statement in ¶ 57 was materially false and misleading at the time it was made because the Company, through its applications, actively sought to put malware on its user's phones.

59. The 2023 Annual Report contained the following risk disclosure about the improper use of data:

> ***Our business generates and processes a large amount of data, and we are required to comply with laws relating to privacy and cybersecurity. The improper use or disclosure of data could have a material and adverse effect on our business and prospects.***
>
> Our business generates and processes a large amount of data. We face a number of challenges relating to data from transactions and other activities on our platforms, including:
>
> - protecting the data in and hosted on our system, including against attacks on our system ***by outside parties or fraudulent behavior or improper use by our employees***, and securely transmitting such data over public networks;

- addressing concerns related to privacy, sharing, safety, security and other factors; and
- ***complying with applicable laws and regulations relating to the collection, use, storage, transfer, disclosure and security of personal data***, including any requests from regulatory and government authorities relating to these data.

To address these challenges, we have adopted strict security policies and measures, including encryption technology, to protect our proprietary data and buyer information. ***Maintaining complete security on our platforms and systems for the storage and transmission of confidential or private data, such as buyers' personal information, payment-related information and transaction information, is essential to maintaining consumer confidence in our platforms and systems.***

However, advances in technology, the expertise of hackers, new discoveries in the field of cryptography or other events or developments could result in a compromise or breach of the technology that we use to protect our data. We may not be able to prevent third parties, especially hackers or other individuals or entities engaging in similar activities through viruses, Trojan horses, malicious software, break-ins, phishing attacks, third-party manipulation or security breaches, from illegally obtaining the confidential or private data we hold on our platforms. Individuals or entities that illegally obtain confidential or private data may further engage in various other illegal activities using such data. The methods used by hackers and others engaging in illegal online activities are increasingly more sophisticated and constantly evolving. In addition, all online payments for products sold on our platforms are settled through third-party payment services. We have limited control or influence over the security policies or measures adopted by third-party providers of online payment services through which some of our buyers may choose to make payment for purchases.

Any negative publicity on our platforms' data safety or privacy protection mechanisms and policies, and any claims asserted or investigations against us or fines imposed upon us as a result of actual or perceived failures, could have a material and adverse effect on our public image, reputation, financial condition and results of operations. Any compromise of our information security or the information security measures of our contracted third-party payment service providers that results in data being improperly used or disclosed could also materially and adversely affect us. Significant capital, managerial and other resources, including costs incurred to deploy additional personnel, develop network protection technologies, train employees, and engage third-party experts and consultants, may be required to ensure and enhance information security or to address the issues caused by a potential security failure.

(Emphasis added).

60. The statement in ¶ 59 was materially false and misleading at the time it was made because it omitted that the Company placed malware on its user's smart phones in order to improperly collect personal data, exposing the Company to heightened regulatory risk.

61. The 2023 Annual Report contained the following risk disclosure about legal risk relating to data privacy:

> ***Our business is subject to complex and evolving laws and regulations regarding privacy and data protection in the countries and regions where we have operations. These laws and regulations can be complex and stringent, and many are subject to change and evolving interpretation, which may result in claims, changes to our data and other business practices, regulatory investigations, penalties, or otherwise affect our business.***
>
> Regulatory authorities around the world have adopted laws and regulations or are considering legislative and regulatory proposals concerning privacy and data protection, including in the PRC, U.S. and the European Union. These laws and regulations regulate the way we collect, use, store, transfer, disclose and secure data and protect the privacy of our users. Global developments in these laws may also create additional compliance obligations for us in the jurisdictions in which we operate.
>
> * * *
>
> In the United States, rules and regulations governing data privacy and security include those promulgated under the authority of the Federal Trade Commission Act, the Electronic Communications Privacy Act, the Computer Fraud and Abuse Act, California's California Consumer Privacy Act of 2018 ("CCPA") and California Privacy Rights Act of 2020 ("CPRA"), and other state and federal laws relating to privacy, consumer protection, and data security. The CCPA and CPRA contain requirements regarding the handling of personal information of California consumers and households, including compliance and record keeping obligations, the right of individuals to request access to and deletion of their personal information, and the right to opt out of the sale and other uses of their personal information, and provide a private right of action and statutory damages for data breaches. Other jurisdictions in the United States are beginning to expand existing regulations, or propose laws similar to the CCPA, which will continue to shape the data privacy environment nationally. Aspects of certain newly enacted state privacy statutes remain unclear, resulting in further legal uncertainty and potentially requiring us to modify our data practices and policies and to incur substantial additional costs and expenses to comply. ***If more stringent privacy legislation arises in the United States, it could increase our potential liability and adversely affect our business, results of operations, and financial condition***.
>
> * * *

> ***Complying with these laws and contractual or other obligations relating to privacy, data protection, data transfers, data localization, or information security may require us to incur substantial operational costs or modify our data practices and policies***. We have taken and will continue to take reasonable measures to comply with such laws and regulations, including those set forth under "Item 4. Information on the Company—B. Business Overview—Data Security and Protection" and "Item 16K. Cybersecurity." ***However, there are uncertainties with respect to how such laws and regulations will be implemented and interpreted in practice. Complying with applicable laws and regulations relating to data security and personal information protection may be costly and result in additional expenses to us, and any material failure to do so may subject us to potential liability, regulatory investigations, costly litigation or negative publicity, harm our reputation and business operations, significantly limit or completely hinder our ability to continue to offer securities to investors, or cause the value of such securities to significantly decline***.
>
> (Emphasis added).

62. The statement in ¶ 61 was materially false and misleading at the time it was made because it understated the Company's legal risk stemming from data privacy issues, considering that the Company placed malware on its user's phones.

63. The 2023 Annual Report contained the following risk disclosure about scrutiny of the Company:

> ***We may increasingly become a target of public scrutiny and anti-competitive actions conducted by competitors or third parties with ill intent, including complaints to regulatory agencies, negative media coverage, and public dissemination of malicious reports or accusations about our business, all of which could severely damage our reputation and materially and adversely affect our business and prospects.***
>
> We process an extremely large number of transactions on a daily basis on our platforms, ***and the high volume of transactions taking place on our platforms as well as publicity about our business create the possibility of heightened attention from the public, competitors, regulators and the media***. Heightened regulatory and public concerns over consumer protection and consumer safety issues may subject us to additional legal and social responsibilities and increased scrutiny and negative publicity over these issues, ***due to the large number of transactions that take place on our platform and the increasing scope of our overall business operations***. In addition, changes in our services or policies have resulted or could result in objections by the public, our competitors, operators of traditional or new media and social networks, merchants on our platform or others. From time to time, these objections or allegations, regardless of their veracity, may result in consumer dissatisfaction, public protests or negative publicity, which could result in government inquiry or substantial harm to our brand, reputation and operations.

> In particular, as the competition in the e-commerce industry further intensifies, we are increasingly susceptible to aggressive, anti-competitive and potentially malicious behaviors, conducts and campaigns by our competitors or third parties with ill intent. For example, untrue and unsubstantiated allegations targeting our platforms or merchants on our platforms may be posted on internet forums, social media platforms or websites by anyone on an anonymous basis. The availability of information on the internet is virtually immediate, as is its impact. These information platforms may not necessarily filter or check the accuracy of information before allowing them to be published. We are often afforded little or no time to respond. For instance, in March 2023, a number of media channels reported cybersecurity concerns about our Pinduoduo mobile app alleged by an anonymous source. Competitors or third parties with ulterior motives could launch aggressive marketing and publicity strategies against us and place the media coverage about this incident among other innocuous or unrelated matters. We are working with stakeholders to refute the allegations while using this opportunity to review our practices. As a result of this anti-competitive conduct, or activities of a similar nature, our brand name and reputation may be materially and adversely affected, and our business operations and strategies may be disrupted or harmed. We may even be subject to governmental or regulatory scrutiny or third-party claims as a result. Meanwhile, we may be required to spend significant amount of time and incur substantial costs to react to or address these consequences. There is no assurance that we will be able to effectively defend ourselves against this type of anti-competitive conduct within a reasonable period of time, or at all.
>
> Moreover, as our business expands and grows, both organically and through acquisitions of and investments in other businesses, we may be exposed to heightened public scrutiny in jurisdictions where we already operate as well as in new jurisdictions where we may operate. There is no assurance that we would not become a target for regulatory or public scrutiny in the future or that scrutiny and public exposure would not severely damage our reputation, business or prospects.
>
> (Emphasis added).

64. The statement in ¶ 63 was materially false and misleading at the time it was made because it stated that the Company could become a target as a result of its scale. In fact, the Company was at increased risk of regulatory and public scrutiny (as well as negative media coverage) due to its malfeasance, including placing malware on its user's smart phones and selling goods that were likely made by forced labor.

65. The 2023 Annual Report contained the following risk disclosure regarding international trade policies:

Changes in U.S. and international trade policies, escalations of tensions in international relations, and increased scrutiny from customs and other authorities, may adversely impact our business and operating results.

There have been heightened tensions in international relations in recent years, which has resulted in and may continue to cause changes in international trade policies and additional barriers to trade. Countries impose, modify, and remove tariffs and other trade restrictions in response to a diverse array of factors, including global and national economic and political conditions, which make it difficult to predict future developments regarding tariffs and other trade restrictions. For example, the tensions between the United States and China in recent years have led to additional or higher tariffs imposed by the United States on certain products imported from China and restrictions on the sale of certain products into the United States. We operate in a number of countries and regions around the world. Tariffs and other restrictions imposed by any country or region we serve could affect our business and financial condition. Trade restrictions, including tariffs, quotas, embargoes, safeguards, and customs restrictions, could restrict our and our merchants' ability to source and sell products to the global markets, could increase our costs or reduce the competitiveness of the prices of products offered on our platforms and could affect our and our merchants' ability to timely ship and deliver products to our buyers, any of which could harm our business, financial condition, and results of operations.

In addition, tensions in the relations between the United States and China, or between other countries, may intensify and the United States, China, or other countries may adopt drastic measures in the future that impact our global business operations. Recent legislative activities in the U.S. regarding, and economic and trade sanctions threatened and/or imposed by the U.S. government on, a number of technology companies with significant China operations have raised concerns as to whether, in the future, there will be additional regulatory challenges or restrictions involving other technology companies with significant China operations. Similar or more expansive restrictions that may be imposed by the United States or other jurisdictions in the future, could materially and adversely affect our business. The adoption or expansion of restrictions, including restrictions or complete bans on access to apps and other platforms, cross-border data transfers, tariffs, or other governmental action related to economic policies, has the potential to adversely impact our business, operational results and financial position.

Currently, certain orders purchased by consumers in the United States from merchants outside of the United States through our Temu platform are imported into the United States under the exemption provided in Section 321 of the Tariff Act of 1930, which exempts packages shipped to the United States under a specified monetary threshold from import duties as long as certain requirements are met. If this exemption were to become unavailable to these orders, or if the exemption threshold were to decrease, our business, financial condition and results of operations may be materially and adversely affected. Additional informational or other procedural requirements may make it slower and more costly to ship packages to the United States, which may affect the business of our Temu platform in the United States. Governments in other jurisdictions may also consider proposals to amend laws and regulations relating to customs that, if adopted, would make

> importing goods into those jurisdictions more complicated, which could adversely affect our business.

66. The statement in ¶ 65 was materially false and misleading at the time it was made because, by the time the 2023 Annual Report was filed with the SEC, the UFLPA had been signed into law and gone into effect. Under the UFLPA, products originating from the Xinjiang region of China imported into the United States must be certified as not being produced by forced labor. Given that the Company shipped goods into the United States from Xinjiang, the UFLPA presented increased risk of difficulties exporting products into the United States from China.

67. The 2023 Annual Report contained the following risk disclosure about legal compliance:

> ***Our business is subject to a large number of laws across many jurisdictions, many of which are evolving.***
>
> We are subject to a variety of laws and regulation across the many jurisdictions where we operate, including without limitation those relating to international trade, investment restrictions, product liability, employment and labor, taxation, consumer protection, marketing and advertising, online payments and money transmission, data privacy and protection, intellectual property protection, trust and safety, and supply chain compliance.
>
> These laws and regulations can be significantly different across different jurisdictions and are continually evolving. Compliance with these laws and regulations is costly, requires significant management time and effort and may require changes to our business practices for local adaptation. Additionally, it is not always clear how these laws and regulations apply to e-commerce platforms as many of them, when enacted, did not address the unique issues that arise in the context of e-commerce platforms. In some jurisdictions, the authorities may seek to impose domestic laws and regulations on our global operations extraterritorially. We may also be subject to inconsistent compliance obligations across jurisdictions. New platform liability laws, potential amendments to existing laws, and ongoing regulatory and judicial interpretation of platform liability laws may impose costs, burdens and uncertainty on us and the merchants on our platforms. To comply with new platform liability laws, we could incur significant costs implementing any required changes, investigating and defending claims and, if we are found liable for any violations of such laws, significant damages. In addition, if legislation or regulatory inquiries, even if focused on other entities, require us to expend significant resources in response or result in the imposition of new obligations, our business and results of operations could be adversely affected.

We strive to comply with all laws and regulations that are applicable to our operations around the world. Despite our efforts, we may not have fully complied in the past, and may not be able to fully or timely comply in the future, with all applicable laws and regulations, particularly where the regulatory regimes have not been broadly applied to e-commerce platforms. We may also be subject to conflicting laws, regulations, rules and orders, where compliance with those of one jurisdiction could result in violation of those of another jurisdiction. Relatedly, in the ordinary course of our business and in light of the scale of our global operations, we are, and will continue to be, regularly subject to formal and informal reviews, queries, investigations, proceedings or other types of administrative actions by governmental and regulatory authorities in the jurisdictions in which we operate under existing laws, regulations, or interpretations or pursuing new and novel approaches to regulate our operations. The number and scale of these proceedings have increased, and will likely continue to increase, as our business has expanded in scope and geographic reach, and as our platforms become more complex, available to, and used by more people, and as governments and regulatory authorities seek to regulate us on a pre-emptive basis. Unfavorable regulations, laws, decisions, or interpretations by government or regulatory authorities applying those laws and regulations, or inquiries, investigations, or enforcement actions threatened or initiated by them could expose us to unanticipated civil and criminal liability or penalties (including substantial monetary fines); subject us to sanctions; harm our brands and reputation; increase our cost of doing business; require us to change the way we operate in a way adverse to our business, including by discontinuing certain services or restricting our operations in one or more jurisdictions; adversely affect our ability to attract merchants and buyers; impede our growth; or otherwise have a material effect on our business. The media, political, and regulatory scrutiny we face, which may continue to increase, amplifies these risks. All of these could materially and adversely affect our business, prospects, financial condition, reputation, and the trading price of our listed securities.

Additionally, if the third-party merchants that sell merchandise on our platforms or the third-party vendors that provide services to us violate applicable laws or regulations, those violations could also result in liabilities for us and harm our brands, reputation and business. For example, in June 2022, the Uyghur Forced Labor Prevention Act, or the UFLPA, became effective in the U.S., establishing a rebuttable presumption that goods mined, produced, or manufactured in a certain region in China or by an entity on the UFLPA Entity List are prohibited from importation into the U.S. We require merchants on the Temu platform to comply with our third-party code of conduct, which strictly prohibits the use of forced, penal or child labor. In addition, we establish policies and procedures to ensure that no seller on the Temu platform is on the UFLPA Entity List, and use technology to identify products that are at higher risk of non-compliance. Any third-party violations of applicable laws or our policies may subject us to negative publicity, investigations, fines, fees, settlements or other costs and liabilities as a result of the enforcement of laws, regulations, sanctions, embargoes, export controls programs or other restrictions. Our ability to rely on insurance, contracts, indemnification and other remedies to limit these liabilities may be insufficient or unavailable in some cases. Furthermore, the circumstances in which we may be held liable for the acts, omissions, or responsibilities of our merchants or other third parties are uncertain, complex, and

> evolving. Upcoming and proposed regulations may require platforms like ours to comply with additional obligations, and the resulting compliance costs and potential liability risk could negatively impact our business.
>
> (Emphasis added).

68. The statement in ¶ 67 was materially false and misleading at the time it was made because the Company did not meaningfully attempt to comply with the UFLPA, among other laws.

69. The statements contained in ¶¶ 22, 24, 26, 28, 31, 33, 35, 37, 39, 42, 44, 46, 48, 50, 52, 54, 57, 59, 61, 63, 65, and 67 were materially false and/or misleading because they misrepresented and failed to disclose the following adverse facts pertaining to the Company's business, operations, and prospects, which were known to Defendants or recklessly disregarded by them. Specifically, Defendants made false and/or misleading statements and/or failed to disclose that: (1) PDD's applications contained malware, which was designed to obtain user data without the user's consent, including reading private text messages; (2) PDD has no meaningful system to prevent goods made by forced labor from being sold on its platform, and has openly sold banned products on its Temu platform; (3) the foregoing subjected the Company to a heightened risk of legal and political scrutiny; and (4) as a result, Defendants' statements about its business, operations, and prospects, were materially false and misleading and/or lacked a reasonable basis at all relevant times.

THE TRUTH BEGINS TO EMERGE
DISCLOSURES RELATING TO MALWARE

70. On March 21, 2023, after market hours, *Reuters* published an article entitled "Google suspends China's Pinduoduo app on security concerns." It stated the following:

> Alphabet Inc's [. . .] ***Google suspended the Play version of [PDD's] Pinduoduo app for security concerns, after malware issues were found on versions of the Chinese e-commerce app outside Google's app store***, a company spokesperson said on Tuesday.
>
> ***"Off-Play versions of this app that have been found to contain malware have been***

> ***enforced on via Google Play Protect," the spokesperson said in a statement, adding that the Play version of the app has been suspended for security concerns.***
>
> ***Google Play Protect scans Android devices with Google Play Services for potentially harmful apps and works to prevent the installation of malicious apps.***
>
> ***"Google Play has informed us this morning that Pinduoduo App has been temporarily suspended as the current version is not compliant with Google's Policy, but has not shared more details,"* a Pinduoduo spokesperson said in an email to Reuters.**
>
> There are several other apps that have been suspended by Google Play, Pinduoduo said, adding that there are multiple reasons an app is temporarily suspended. Google did not immediately respond to a query on the suspension of other apps on the Play store.
>
> * * *
>
> The development comes amid efforts by the U.S. government to bolster its cyber defenses in the face of a steady increase in hacking and digital crimes targeting the country.
>
> The government recently announced a new cybersecurity strategy that named China and Russia as the most prominent threats to the United States.
>
> (Emphasis added).

71. On this news, the price of PDD ADS' declined by $3.35 per share, or 4.24%, to close at $75.58 on March 22, 2023.

72. On March 27, 2023, before the market opened, Bloomberg published an article entitled "Pinduoduo App Malware detailed by Cybersecurity Researchers." (the "Bloomberg Article").

73. The Bloomberg Article stated that "[s]ecurity researchers at Moscow-based Kaspersky Lab have identified and outlined potential malware in versions of [PDD's] Chinese shopping app Pinduoduo, days after Google suspended it from its Android app store." It then stated the following:

> In one of the first public accountings of the malicious code, Kaspersky laid out how the app could elevate its own privileges to undermine use privacy and data security. It tested versions of the app distributed through a local app store in China, where [Huawei], [Tencent] and Xiaomi Corp. run some of the biggest app markets.

> Kaspersky's findings, shared with Bloomberg News, were among the clearest explanations from an independent security team for what triggered Google's action and malware warning last week. ***The cybersecurity firm, which has played a role in uncovering some of the biggest cyberattacks in history, said it found evidence that earlier versions of Pinduoduo exploited system software vulnerabilities to install backdoors and gain unauthorized access to user data and notifications***.
>
> Those conclusions agreed in large part with those of researchers that had posted their discoveries online in past weeks, though Bloomberg News hasn't verified the authenticity of the earlier reports.
>
> (Emphasis added).

74. The Bloomberg Article quoted Igor Golovin, a Kaspersky security researcher, as saying that "[s]ome versions of the Pinduoduo app contained malicious code, which exploited known Android vulnerabilities to escalate privileges, download and execute additional malicious modules, some of which also gained access to users' notifications and files[.]"

75. On this news, the price of PDD ADS' went down by $2.28 per share, or 3.08%, to close at $71.68 on March 27, 2023.

76. Then, on Sunday April 2, 2023, CNN published an article entitled "'I've never seen anything like this:' One of China's most popular apps has the ability to spy on its users, say experts." (the "CNN Article"). The CNN Article, which was updated on April 3, 2023, stated the following:

> It is one of China's most popular shopping apps, selling clothing, groceries and just about everything else under the sun to more than 750 million users a month.
>
> But according to cybersecurity researchers, ***it can also bypass users' cell phone security to monitor activities on other apps, check notifications, read private messages and change settings***.
>
> And once installed, it's tough to remove.
>
> ***While many apps collect vast troves of user data, sometimes without explicit consent, experts say e-commerce giant Pinduoduo has taken violations of privacy and data security to the next level***.

* * *

Malware, short for malicious software, refers to any software developed to steal data or interfere with computer systems and mobile devices.

Evidence of sophisticated malware in the Pinduoduo app comes amid intense scrutiny of Chinese-developed apps like TikTok over concerns about data security.

* * *

The revelations are also likely to draw more attention to Pinduoduo's international sister app, Temu, which is topping US download charts and fast expanding in other Western markets. Both are owned by Nasdaq-listed PDD, a multinational company with roots in China.

While Temu has not been implicated, Pinduoduo's alleged actions risk casting a shadow over its sister app's global expansion.

There is no evidence that Pinduoduo has handed data to the Chinese government. But as Beijing enjoys significant leverage over businesses under its jurisdiction, there are concerns from US lawmakers that any company operating in China could be forced to cooperate with a broad range of security activities.

The findings follow Google's suspension of Pinduoduo from its Play Store in March, citing malware identified in versions of the app.

An ensuing report from Bloomberg said a Russian cybersecurity firm had also identified potential malware in the app.

Pinduoduo has previously rejected "the speculation and accusation that Pinduoduo app is malicious."

CNN has contacted PDD multiple times over email and phone for comment, but has not received a response.

(Emphasis added).

77. The CNN Article stated the following about the reports CNN received from cybersecurity experts about PDD's applications:

In a detailed investigation, CNN spoke to half a dozen cybersecurity teams from Asia, Europe and the United States — as well as multiple former and current Pinduoduo employees — after receiving a tipoff.

Multiple experts identified the presence of malware on the Pinduoduo app that exploited vulnerabilities in Android operating systems. Company insiders said the exploits were utilized to spy on users and competitors, allegedly to boost sales.

"***We haven't seen a mainstream app like this trying to escalate their privileges to gain access to things that they're not supposed to gain access to***," said Mikko Hyppönen, chief research officer at WithSecure, a Finnish cybersecurity firm.

"***This is highly unusual, and it is pretty damning for Pinduoduo***."

* * *

Approached by CNN, researchers from Tel Aviv-based cyber firm Check Point Research, Delaware-based app security startup Oversecured and Hyppönen's WithSecure conducted independent analysis of the 6.49.0 version of the app, released on Chinese app stores in late February.
Google Play is not available in China, and Android users in the country download their apps from local stores. In March, when Google suspended Pinduoduo, it said it had found malware in off-Play versions of the app.

The researchers found code designed to achieve "privilege escalation": a type of cyberattack that exploits a vulnerable operating system to gain a higher level of access to data than it's supposed to have, according to experts.

"***Our team has reverse engineered that code and we can confirm that it tries to escalate rights, tries to gain access to things normal apps wouldn't be able to do on Android phones***," said Hyppönen.

The app was able to continue running in the background and prevent itself from being uninstalled, which allowed it to boost its monthly active user rates, Hyppönen said. It also had the ability to spy on competitors by tracking activity on other shopping apps and getting information from them, he added.

Check Point Research additionally identified ways in which the app was able to evade scrutiny.

The app deployed a method that allowed it to push updates without an app store review process meant to detect malicious applications, the researchers said.

They also identified in some plug-ins the intent to obscure potentially malicious components by hiding them under legitimate file names, such as Google's.

"Such a technique is widely used by malware developers that inject malicious code into applications that have legitimate functionality," they said.

(Emphasis added).

78. The CNN Article stated the following about how a Pinduoduo employee had stated that PDD for years had a team that worked to exploit vulnerabilities in phones that operate on the Android system:

> It was in 2020, ***according to a current Pinduoduo employee, that the company set up a team of about 100 engineers and product managers to dig for vulnerabilities in Android phones, develop ways to exploit them — and turn that into profit***.
>
> According to the source, ***who requested anonymity for fear of reprisals, the company only targeted users in rural areas and smaller towns initially, while avoiding users in megacities such as Beijing and Shanghai***.
>
> "***The goal was to reduce the risk of being exposed***," they said.
>
> By collecting expansive data on user activities, the company was able to create a comprehensive portrait of users' habits, interests and preferences, according to the source.
>
> This allowed it to improve its machine learning model to offer more personalized push notifications and ads, attracting users to open the app and place orders, they said.
>
> ***The team was disbanded in early March, the source added, after questions about their activities came to light***.
>
> PDD didn't reply to CNN's repeated requests for comment on the team.
>
> (Emphasis added).

79. The CNN Article stated, in pertinent part, the following about how the team working to exploit vulnerabilities in the Android system had been, at least partially, disbanded:

> Soon after, on March 5, Pinduoduo issued a new update of its app, version 6.50.0, ***which removed the exploits, according to two experts who CNN spoke to***.
>
> ***Two days after the update, Pinduoduo disbanded the team of engineers and product managers who had developed the exploits***, according to the Pinduoduo source.
>
> ***The next day, team members found themselves locked out of Pinduoduo's bespoke workplace communication app, Knock, and lost access to files on the company's internal network***. Engineers also found their access to big data, data sheets and the log system revoked, the source said.

> ***Most of the team were transferred to work at Temu. They were assigned to different departments at the subsidiary***, with some working on marketing or developing push notifications, according to the source.
>
> ***A core group of about 20 cybersecurity engineers who specialize in finding and exploiting vulnerabilities remain at Pinduoduo***, they said.
>
> Toshin of Oversecured, who looked into the update, said although the exploits were removed, the underlying code was still there and could be reactivated to carry out attacks.
>
> (Emphasis added).

80. The CNN Article further stated the following about how Android had been targeted:

> In China, about three quarters of smartphone users are on the Android system. Apple (AAPL)'s iPhone has 25% market share, according to Daniel Ives of Wedbush Securities.
>
> Sergey Toshin, the founder of Oversecured, said ***Pinduoduo's malware specifically targeted different Android-based operating systems, including those used by Samsung, Huawei, Xiaomi and Oppo***.
>
> CNN has reached out to these companies for comment.
>
> ***Toshin described Pinduoduo as "the most dangerous malware" ever found among mainstream apps***.
>
> "I've never seen anything like this before. It's like, super expansive," he said.
>
> Most phone manufacturers globally customize the core Android software, the Android Open Source Project (AOSP), to add unique features and applications to their own devices.
>
> ***Toshin found Pinduoduo to have exploited about 50 Android system vulnerabilities***. Most of the exploits were tailor made for customized parts known as the original equipment manufacturer (OEM) code, which tends to be audited less often than AOSP and is therefore more prone to vulnerabilities, he said.
>
> Pinduoduo also exploited a number of AOSP vulnerabilities, including one which was flagged by Toshin to Google in February 2022. Google fixed the bug this March, he said.
>
> According to Toshin, the exploits allowed Pinduoduo access to users' locations, contacts, calendars, notifications and photo albums without their consent. They were also able to change system settings and access users' social network accounts and chats, he said.

> Of the six teams CNN spoke to for this story, three did not conduct full examinations. But their primary reviews showed that Pinduoduo asked for a large number of permissions beyond the normal functions of a shopping app.
>
> They included "potentially invasive permissions" such as "set wallpaper" and "download without notification," said René Mayrhofer, head of the Institute of Networks and Security at the Johannes Kepler University Linz in Austria.
>
> (Emphasis added).

81. On this news, the price of PDD ADS' declined $1.06 per share compared to the prior closing price, or 1.4%, to close at $74.84 on April 3, 2023. The next day, PDD ADS' declined a further $1.64, or 2.19%, to close at $73.20.

82. Then, on June 25, 2024, Tim Griffin, the Attorney General of Arkansas, issued a release in which he announced that he is suing Temu for violations of the Arkansas Deceptive Trade Practices Act ("ADTPA") and the Arkansas Personal Information Protection Act ("PIPA").

83. The announcement quoted AG Griffin as saying, in pertinent part, the following:

> ***Temu is not an online marketplace like Amazon or Walmart. It is a data-theft business that sells goods online as a means to an end***. Today I have filed a first-of-its-kind state lawsuit against the parent companies of Temu—PDD Holdings Inc. and WhaleCo Inc.—for violating the ADTPA and PIPA. ***Though it is known as an e-commerce platform, Temu is functionally malware and spyware. It is purposefully designed to gain unrestricted access to a user's phone operating system***. It can override data privacy settings on users' devices, and it monetizes this unauthorized collection of data.
>
> While this is the first state lawsuit against Temu over its deceptive trade practices, it is not the first time Temu's tactics have been called into question.
>
> (Emphasis added).

84. On the same day, the lawsuit, captioned *State of Arkansas v. PDD Holdings Inc. F/K/A Pinduoduo Inc..; and WhaleCo Inc. D/B/A Temu,* Case No. 12-cv-24-149, was filed in the Circuit Court of Cleburne County, Arkansas (the "Arkansas Complaint").

85. The Arkansas Complaint alleged violations of the Arkansas Deceptive Trade Practices Act and the Arkansas Personal Information Protection Act, and that the Company had engaged in Unjust Enrichment.

86. The Arkansas Complaint said the following about Temu:

> Temu is purposefully designed to gain unrestricted access to a user's phone operating system, including, but not limited to, a user's camera, specific location, contacts, text messages, documents, and other applications. Temu is designed to make this expansive access undetected, even by sophisticated users. Once installed, Temu can recompile itself and change properties, including overriding the data privacy settings users believe they have in place. Even users without the Temu app are subject to Temu's gross overreach if any of their information is on the phone of a Temu user. Temu monetizes this unauthorized collection of data by selling it to third parties, profiting at the direct expense of Arkansans' privacy rights.

87. On this news, PDD's ADS' fell by 1.26% on June 26, 2024, and 4.55% on June 27, 2024.

DISCLOSURES RELATED TO FORCED LABOR

88. On June 22, 2023, The New York Times published an article entitled "Congress Spotlights 'Serious' Forced Labor Concerns With Chinese Shopping Sites", which discussed findings by the U.S. House of Representatives' Select Committee on the Chinese Communist Party (the "Committee").

89. The article noted that in 2022, "***the U.S. imposed a ban on products from Xinjiang, citing the region's use of forced labor in factories and mines***." (Emphasis added).

90. Regarding Xinjiang, the article further stated the following regarding the U.S. governments view of materials from the region, given the Chinese government's repressive conduct towards the local Uyghur population:

> The Chinese government has carried out a crackdown in Xinjiang on Uyghurs and other ethnic minorities, including the organized use of forced labor to pick cotton; work in mines; and manufacture electronics, polysilicon and car parts. ***Because of this, the U.S.***

> ***government now presumes all materials from the region to be made with forced labor unless proved otherwise***.
>
> (Emphasis added).

91. It further stated the following about bipartisan findings from the U.S. House of Representatives regarding Temu and the flow of goods made with forced labor from Xinjiang into the United States:

> Lawmakers are flagging what they say are likely significant violations of U.S. Law by Temu, a popular Chinese shopping platform, ***accusing it of providing an unchecked channel that allows goods made with forced labor to flow into the United States.***
>
> In a report released Thursday, the House Select Committee on the Chinese Communist Party said Temu, a rapidly growing side that sells electronics, makeup, toys and clothing, ***had failed "to maintain even the façade of a meaningful compliance program" for its supply chains and was likely shipping products made with forced labor into the United States on a "regular basis."***
>
> The report stems from a continuing investigation into forced labor in supply chains that touch on China. Lawmakers said the report was based on responses submitted to the committee by Temu[.]
>
> The report offered a particularly scathing assessment of Temu, saying there is an "extremely high risk that Temu's supply chains are contaminated with forced labor."
>
> (Emphasis added).

92. The New York Times article quoted Representative Mike Gallagher, a former Republican member of congress who led the Committee, as saying that "***Temu is doing next to nothing to keep its supply chains free from slave labor***[.] At the same time, [Temu is] building empires around the de minimis loophole in our import rules: dodging import taxes and evading scrutiny on the millions of goods they sell to Americans." (Emphasis added).

93. The article referred to the importing method as one that allows companies "to bring products into the United States duty-free and with less scrutiny from customs, as long as packages

are sent directly to consumers and valued at under $800. lawmakers have been pushing to close off this shipping channel, which is called de minimus, for companies sourcing goods from China."

94. The article further stated the following about the consequences of the de minimus rule, which Temu makes "heavy use of":

> De minimus shipping [. . .] requires far less information to be disclosed about the products and the companies involved in the transaction, making it harder for U.S. customs officials to detect packages with narcotics, counterfeits and goods made with forced labor.

95. The Committee's report, which was also released on June 22, 2023, was entitled "Fast Fashion and the Uyghur Genocide: Interim Findings" (the Committee Report"). As noted in the Committee Report, the Committee had requested information (including through questions and document production) from Temu, in order to assess its efforts to comply with the Uyghur Forced Labor Prevention Act (the "UFLPA").

96. The Committee Report stated the following, in pertinent part, about the de minimus loophole:

> The Committee asked questions related to [Temu's] use of Section 321 of the Tariff Act of 1930, known as the de minimis rule, which allows importers to avoid customs duties on incoming packages that are valued at less than $800. In addition, because of the of the overwhelming volume of small packages and lack of actionable data, 'in 2022, CBP cleared over 685 million de minimis shipments with insufficient data to properly determine risk."

97. The Committee Report further stated that "Temu does not have any system to ensure compliance with the [UFLPA]. ***This all but guarantees that shipments from Temu containing products made with forced labor are entering the United States on a regular basis, in violation of the UFLPA***." (Emphasis added).

98. The Committee Report further stated that "Temu's business model, which relies on the de minimis provision, is to avoid bearing responsibility for compliance with the UFLPA

and other prohibitions on forced labor while relying on tens of thousands of Chinese suppliers to ship goods direct to U.S. customers."

99. The Committee Report stated that the "***only measure*** Temu reported that it takes to ensure that it is not shipping goods to Americans that are produced with forced labor in violation of U.S. law was ***that its suppliers agree to boilerplate terms and conditions that prohibit the use of forced labor***." Further, the Committee Report stated that "Temu admitted that it '***does not expressly prohibit third-party sellers from selling products based on their origin in the Xinjiang Autonomous Region***.'" (Emphasis added).

100. The Committee Report further stated the following:

> The fact that tens of millions of shipments from China are not being sufficiently vetted for UFLPA compliance is contrary to the goals of this landmark legislation. ***The UFLPA creates a presumption that goods mined, produced, or manufactured wholly or in part in Xinjiang (or by designated companies in China) simply may not be imported into the U.S. To rebut this presumption, an importer must meet the high burden of clear and convincing evidence***. The UFLPA also established a UFLPA Entity List, which identifies – and restricts importing from – companies working with the government of Xinjiang on forced labor matters. As discussed at our recent hearing, this law was Congress's direct response to the CCP's use of Uyghur forced labor, with the intent of ensuring that American consumers are not complicit in these ongoing abuses.
>
> (Emphasis added).

101. The Committee Report further stated:

> In light of the sheer volume of shipments sent to the United States through its website, Temu's failure to take any meaningful steps with respect to preventing the importation of goods produced with forced labor is striking. ***Simply put, Temu denies responsibility for ensuring that its 80,000, mostly China-based sellers do not sell products produced with forced labor because Temu is "not the importer of record with respect to goods shipped to the United States."***
>
> ***Despite facilitating millions of purchases by Americans each year, when asked, Temu did not report any compliance or auditing system to independently verify that the tens of thousands of sellers who list on Temu are not selling products produced with Uyghur forced labor***. Temu's current compliance plan relies almost entirely on its China-based third-party sellers that send shipments to the United States with insufficient data to facilitate appropriate customs scrutiny."

> The sole measure that Temu reported that it takes to ensure that it is not selling goods produced with forced labor is to require its sellers to agree with its website's "Third Party Code of Conduct," which includes boilerplate language that the company has "a zero-tolerance policy" for the use of forced, indentured, or penal labor. ***It makes no mention of Xinjiang, the UFLPA, or any other provision of law."***
>
> Despite a valuation estimated at $100 billion, Temu also does not have an auditing or compliance program to determine whether its suppliers are compliant with the Code of Conduct or to verify whether its China-based sellers are in fact complying with the UFLPA and other prohibitions under U.S. law.
>
> (Emphasis added).

102. The Committee Report stated that "Temu relies on a 'reporting system' in which 'consumers, sellers, [and] regulators,' among others, can 'file complaints for violations of Temu platform rules.'" However, "[u]nsurprisingly, 'Temu has not received any complaints concerning forced labor practices.' ***This lack of any complaints highlights the dubious nature of a system that relies solely on external reporting***." (Emphasis added).

103. Specifically, the Committee Report stated that ***"[i]ndividuals and entities in China that raise questions about forced labor are routinely penalized and are unlikely to self-report violations of U.S. law***. It is also unclear how American consumers would have relevant information regarding whether or not a product they purchased on Temu was produced through forced labor or with illicit Xinjiang inputs." (Emphasis added).

104. The Committee Report further stated that the Committee's investigation revealed that the Company was selling a "New Handmade Knitted Cotton Pendant with Xinjiang Cotton." The Committee obtained a screenshot of the product (as seen below), and stated that "[t]he reference to Xinjiang may refer to the materials, the supplier, the pattern, or the origin of the product. ***As discussed at the [Committee's] recent hearing, Xinjiang's cotton industry is intrinsically lined to forced labor and import of such cotton into the U.S. is functionally***

prohibited under U.S. law." (Emphasis added). The Committee Report included the following screenshot from Temu's website:

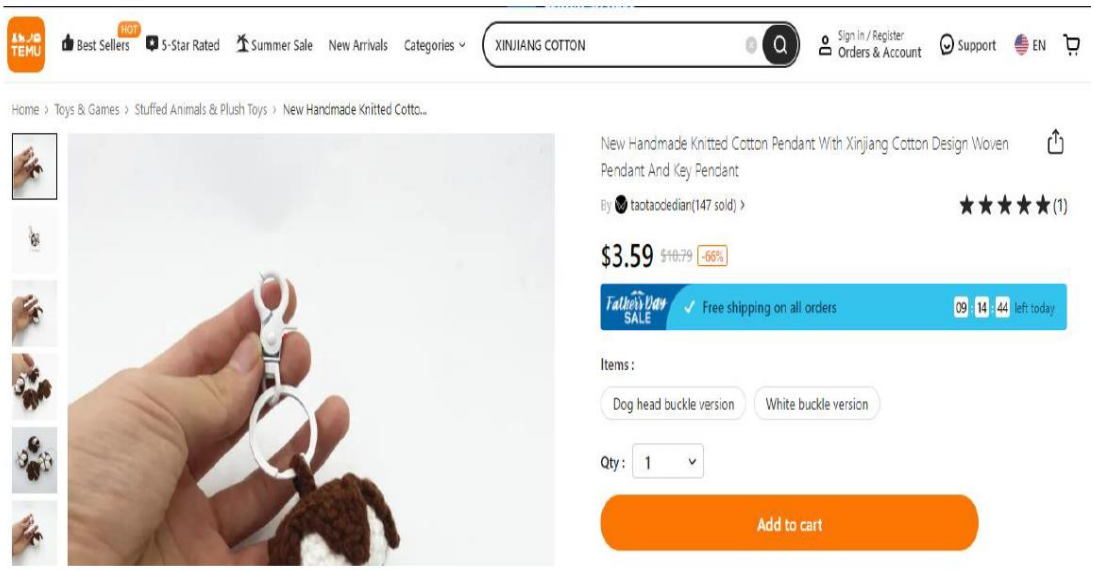

Figure 5: Screenshot of item listed on Temu described as a pendant with "Xinjiang Cotton."

105. Then, on June 23, 2023, during market hours, *Business Insider* published an article entitled "Temu reportedly relies on customers and suppliers to report if goods from the site were produced by forced labor." The Business Insider article reported on the Committee's investigation and findings.

106. On this news, PDD's ADS' fell by $3.09, or 4.24%, to close at $69.80 per ADS on June 23, 2023.

107. Then, on February 12, 2024, after the market closed, Fox Business published an article entitled "Temu's Super Bowl ads spark backlash over China-based firm's forced labor allegations." The article illustrated the increased attention from American lawmakers on Temu and PDD, stating the following:

> Fast fashion retailer Temu's Super Bowl ads drew the ire of lawmakers in Congress over the China-based company's links to products made with the use of forced labor in Xinjiang as well as its data-sharing policies.
>
> Temu, which is linked to e-commerce firm Pinduoduo through their shared parent company PDD Holdings, ran several ads that encouraged viewers to download its app so they can "shop like a billionaire" and be eligible for $10 million in giveaways on the site.
>
> * * *
>
> Members of Congress took to social media to call out Temu's data practices and links to forced labor in China as they sought to advise American consumers against downloading the app.
>
> * * *
>
> Rep. Michelle Steel, R-Calif., who is a member of the House Select Committee on Strategic Competition between the U.S. and the Chinese Communist Party, wrote: "***It's Super Bowl Sunday! While you're watching this game, keep an eye out for ads from Temu, a company profiting from CCP slave labor***. This company should not allowed to profit by manipulating American consumers."
>
> * * *
>
> Chairman of the House Select Committee on the Strategic Competition between the U.S. and the Chinese Communist Party Mike Gallagher, R-Wisc., told FOX Business: "***It's disappointing to see broadcasters turn a blind eye to Temu's comprehensive failure to prevent Uyghur forced labor in its supply chains***. Companies complicit in the Uyghur genocide should have no place in primetime ad slots."
>
> In June 2023, the select committee announced the interim findings from an investigation into links between Temu[,] and products made with forced labor from Uyghurs and other persecuted ethnic minorities in China's Xinjiang province.
>
> (Emphasis added).

108. On this news, PDD's ADS' fell by $2.53 per ADS, or 1.92%, to close at $129.04 per ADS on February 13, 2024.

109. Then, on February 23, 2024, during market hours, *The Information* published an article entitled "U.S. Lawmakers Demand Temu Shipment Ban Over Forced Labor Concerns." In pertinent part, it stated the following:

A number of U.S. lawmakers are pushing for a ban on imports of goods sold on Temu, the fast-growing shopping site known for selling bargain products shipped from China, saying it hasn't done enough to prevent its suppliers from using forced labor, two people with knowledge of the conversations said.
In recent weeks, China critics including Rep. Blaine Luetkemeyer have been asking agencies ***including the Department of Homeland Security to add Temu to a list of violators of the Uyghur Forced Labor Prevention Act, one of the people said. Being on that list amounts to an import ban that would cripple Temu's U.S. business***.

The mounting demands highlight how Temu, which is owned by Chinese e-commerce giant PDD Holdings, has become a high-profile target for U.S. lawmakers as they've stepped up their scrutiny of companies with ties to China over the past year, thanks to its explosive growth with U.S. shoppers and a marketing blitz including Super Bowl television ads earlier this month.

Adding Temu to the UFLPA list would be an unprecedented move, because no retailers or marketplaces have been included yet. Signed into law in late 2021, the UFLPA is meant to ban imports from China's Xinjiang region, where the U.S. has alleged China is employing forced labor through imprisonment of Uyghurs and other ethnic minorities. Beijing has denied any human rights abuses. Temu didn't respond to a request for comment.

So far, the list is made up of manufacturers and other companies that are either based in Xinjiang or the U.S. has alleged use forced labor from Xinjiang. There is also a category for companies that export banned goods but do not manufacture them directly, but the agencies that manage the list have not yet named any violators in this category.

* * *

Last May, a special House committee focused on China asked [Temu to detail its efforts] to comply with the UFLPA. Temu, which operates primarily as a platform for outside sellers, told the committee it shouldn't be subject to the law, since its suppliers, not Temu itself, are the ones importing goods to the U.S. [. . .]

But in a report released in June, the committee found that Temu did not have any system to ensure compliance with the UFLPA, which it said "all but guarantees" that shipments from Temu containing products made with forced labor are entering the U.S. on a regular basis. The committee also said the lack of complaints showed the "dubious nature" of Temu's system for reporting violations.

The pressure on Temu has ramped up even more since then, in particular following the multiple ads it aired during the Super Bowl broadcast earlier this month. ***That's led lawmakers to put more pressure on government agencies, in particular the Department of Homeland Security, to name Temu as a UFLPA violator***, the two people familiar with the discussions said. Only one of the seven agencies in the DHS-chaired Forced Labor

> Enforcement Task Force can make nominations to the list. The DHS didn't have a comment.
>
> "***Temu must be added to the UFLPA Entity List" if it doesn't put systems in place to ensure products entering the U.S. comply with the law***, Rep. Carol Miller said in a statement on Thursday.
>
> ***Other lawmakers including Sen. Roger Marshall and Sen. Mike Braun are trying to drum up support to pressure the agencies to act***, one of the people said. Marshall's office and Braun's office didn't respond to requests for comment.
>
> Lawmakers have also stepped up their public criticism of Temu in recent weeks. Earlier this month, Marshall and Braun published a joint letter they sent to Paramount and CBS asking them not to air Temu's ads during the Super Bowl. And Luetkemeyer earlier this month questioned an official from the Treasury Department, one of the agencies responsible for the list, on why Temu has not been designated as a violator.
>
> (Emphasis added).

110. As a result of Defendants' wrongful acts and omissions, and the precipitous decline in the market value of the Company's common shares, Plaintiff and other Class members have suffered significant losses and damages.

PLAINTIFF'S CLASS ACTION ALLEGATIONS

111. Plaintiff brings this action as a class action pursuant to Federal Rule of Civil Procedure 23(a) and (b)(3) on behalf of a class consisting of all persons other than defendants who acquired the Company's securities publicly traded on NASDAQ during the Class Period, and who were damaged thereby (the "Class"). Excluded from the Class are Defendants, the officers and directors of the Company, members of the Individual Defendants' immediate families and their legal representatives, heirs, successors or assigns and any entity in which Defendants have or had a controlling interest.

112. The members of the Class are so numerous that joinder of all members is impracticable. Throughout the Class Period, the Company's securities were actively traded on NASDAQ. While the exact number of Class members is unknown to Plaintiff at this time and can

be ascertained only through appropriate discovery, Plaintiff believes that there are hundreds, if not thousands of members in the proposed Class.

113. Plaintiff's claims are typical of the claims of the members of the Class as all members of the Class are similarly affected by Defendants' wrongful conduct in violation of federal law that is complained of herein.

114. Plaintiff will fairly and adequately protect the interests of the members of the Class and has retained counsel competent and experienced in class and securities litigation. Plaintiff has no interests antagonistic to or in conflict with those of the Class.

115. Common questions of law and fact exist as to all members of the Class and predominate over any questions solely affecting individual members of the Class. Among the questions of law and fact common to the Class are:

- whether the Exchange Act was violated by Defendants' acts as alleged herein;
- whether statements made by Defendants to the investing public during the Class Period misrepresented material facts about the business and financial condition of the Company;
- whether Defendants' public statements to the investing public during the Class Period omitted material facts necessary to make the statements made, in light of the circumstances under which they were made, not misleading;
- whether the Defendants caused the Company to issue false and misleading filings during the Class Period;
- whether Defendants acted knowingly or recklessly in issuing false filings;
- whether the prices of the Company securities during the Class Period were artificially inflated because of the Defendants' conduct complained of herein; and

- whether the members of the Class have sustained damages and, if so, what is the proper measure of damages.

116. A class action is superior to all other available methods for the fair and efficient adjudication of this controversy since joinder of all members is impracticable. Furthermore, as the damages suffered by individual Class members may be relatively small, the expense and burden of individual litigation make it impossible for members of the Class to individually redress the wrongs done to them. There will be no difficulty in the management of this action as a class action.

117. Plaintiff will rely, in part, upon the presumption of reliance established by the fraud-on-the-market doctrine in that:

- the Company's shares met the requirements for listing, and were listed and actively traded on NASDAQ, an efficient market;
- as a public issuer, the Company filed periodic public reports;
- the Company regularly communicated with public investors via established market communication mechanisms, including through the regular dissemination of press releases via major newswire services and through other wide-ranging public disclosures, such as communications with the financial press and other similar reporting services;
- the Company's ADSs were liquid and traded with moderate to heavy volume during the Class Period; and
- the Company was followed by a number of securities analysts employed by major brokerage firms who wrote reports that were widely distributed and publicly available.

118. Based on the foregoing, the market for the Company's ADSs promptly digested current information regarding the Company from all publicly available sources and reflected such information in the prices of the shares, and Plaintiff and the members of the Class are entitled to a presumption of reliance upon the integrity of the market.

119. Alternatively, Plaintiff and the members of the Class are entitled to the presumption of reliance established by the Supreme Court in *Affiliated Ute Citizens of the State of Utah v. United States*, 406 U.S. 128 (1972), as Defendants omitted material information in their Class Period statements in violation of a duty to disclose such information as detailed above.

COUNT I
For Violations of Section 10(b) And Rule 10b-5 Promulgated Thereunder
Against All Defendants

120. Plaintiff repeats and realleges each and every allegation contained above as if fully set forth herein.

121. This Count is asserted against Defendants is based upon Section 10(b) of the Exchange Act, 15 U.S.C. § 78j(b), and Rule 10b-5 promulgated thereunder by the SEC.

122. During the Class Period, Defendants, individually and in concert, directly or indirectly, disseminated or approved the false statements specified above, which they knew or deliberately disregarded were misleading in that they contained misrepresentations and failed to disclose material facts necessary in order to make the statements made, in light of the circumstances under which they were made, not misleading.

123. Defendants violated §10(b) of the 1934 Act and Rule 10b-5 in that they:

- employed devices, schemes and artifices to defraud;
- made untrue statements of material facts or omitted to state material facts necessary in order to make the statements made, in light of the circumstances under which they were made, not misleading; or

- engaged in acts, practices and a course of business that operated as a fraud or deceit upon plaintiff and others similarly situated in connection with their purchases of the Company's securities during the Class Period.

124. Defendants acted with scienter in that they knew that the public documents and statements issued or disseminated in the name of the Company were materially false and misleading; knew that such statements or documents would be issued or disseminated to the investing public; and knowingly and substantially participated, or acquiesced in the issuance or dissemination of such statements or documents as primary violations of the securities laws. These defendants by virtue of their receipt of information reflecting the true facts of the Company, their control over, and/or receipt and/or modification of the Company's allegedly materially misleading statements, and/or their associations with the Company which made them privy to confidential proprietary information concerning the Company, participated in the fraudulent scheme alleged herein.

125. Individual Defendants, who are the senior officers of the Company, had actual knowledge of the material omissions and/or the falsity of the material statements set forth above, and intended to deceive Plaintiff and the other members of the Class, or, in the alternative, acted with reckless disregard for the truth when they failed to ascertain and disclose the true facts in the statements made by them or any other of the Company's personnel to members of the investing public, including Plaintiff and the Class.

126. As a result of the foregoing, the market price of the Company's securities was artificially inflated during the Class Period. In ignorance of the falsity of Defendants' statements, Plaintiff and the other members of the Class relied on the statements described above and/or the integrity of the market price of the Company's securities during the Class Period in purchasing

the Company's securities at prices that were artificially inflated as a result of Defendants' false and misleading statements.

127. Had Plaintiff and the other members of the Class been aware that the market price of the Company's securities had been artificially and falsely inflated by Defendants' misleading statements and by the material adverse information which Defendants did not disclose, they would not have purchased the Company's securities at the artificially inflated prices that they did, or at all.

128. As a result of the wrongful conduct alleged herein, Plaintiff and other members of the Class have suffered damages in an amount to be established at trial.

129. By reason of the foregoing, Defendants have violated Section 10(b) of the 1934 Act and Rule 10b-5 promulgated thereunder and are liable to the plaintiff and the other members of the Class for substantial damages which they suffered in connection with their purchase of the Company's securities during the Class Period.

COUNT II
Violations of Section 20(a) of the Exchange Act
Against the Individual Defendants

130. Plaintiff repeats and realleges each and every allegation contained in the foregoing paragraphs as if fully set forth herein.

131. During the Class Period, the Individual Defendants participated in the operation and management of the Company, and conducted and participated, directly and indirectly, in the conduct of the Company's business affairs. Because of their senior positions, they knew the adverse non-public information about the Company's business practices.

132. As officers of a publicly owned company, the Individual Defendants had a duty to disseminate accurate and truthful information with respect to the Company's' financial condition

and results of operations, and to correct promptly any public statements issued by the Company which had become materially false or misleading.

133. Because of their positions of control and authority as senior officers, the Individual Defendants were able to, and did, control the contents of the various reports, press releases and public filings which the Company disseminated in the marketplace during the Class Period concerning the Company's results of operations. Throughout the Class Period, the Individual Defendants exercised their power and authority to cause the Company to engage in the wrongful acts complained of herein. The Individual Defendants therefore, were "controlling persons" of the Company within the meaning of Section 20(a) of the Exchange Act. In this capacity, they participated in the unlawful conduct alleged which artificially inflated the market price of the Company's securities.

134. By reason of the above conduct, the Individual Defendants are liable pursuant to Section 20(a) of the Exchange Act for the violations committed by the Company.

PRAYER FOR RELIEF

WHEREFORE, plaintiff, on behalf of himself and the Class, prays for judgment and relief as follows:

(a) declaring this action to be a proper class action, designating plaintiff as Lead Plaintiff and certifying plaintiff as a class representative under Rule 23 of the Federal Rules of Civil Procedure and designating plaintiff's counsel as Lead Counsel;

(b) awarding damages in favor of plaintiff and the other Class members against all defendants, jointly and severally, together with interest thereon;

awarding plaintiff and the Class reasonable costs and expenses incurred in this action, including counsel fees and expert fees; and

(d) awarding plaintiff and other members of the Class such other and further relief as the Court may deem just and proper.

JURY TRIAL DEMANDED

Plaintiff hereby demands a trial by jury.

Dated: August 13, 2024

THE ROSEN LAW FIRM, P.A.
/s/ Phillip Kim
Phillip Kim, Esq.
Laurence M. Rosen, Esq.
275 Madison Avenue, 40th Floor
New York, NY 10016
Telephone: (212) 686-1060
Fax: (212) 202-3827
Email: philkim@rosenlegal.com
lrosen@rosenlegal.com

Counsel for Plaintiff